Leçons tirées d'une récente restauration post-rançongiciel

Découvrez comment une entreprise de fabrication internationale a rapidement restauré Active Directory suite à une attaque par rançongiciel.

Quest

Introduction

Les stratégies de restauration suite à une attaque par rançongiciel, c'est bien en théorie, mais c'est encore mieux en pratique, en apprenant d'expériences concrètes. Ce livre blanc explore les leçons essentielles qu'une entreprise internationale du secteur de la fabrication a apprises pendant une restauration d'Active Directory réussie suite à une attaque par rançongiciel.

Chaque entreprise doit se préparer à l'éventualité d'une attaque par rançongiciel.

Les titres actuels montrent que le monde informatique peut être un monde dangereux. Les entreprises de tous bords subissent des attaques par rançongiciels dévastatrices. Certaines des organisations les plus connues incluent Colonial Pipeline, JBS et Kaseya. Malheureusement, le problème ne se limite pas aux grandes entreprises : les PME, les administrations, les districts scolaires, les fournisseurs de soins de santé et bien d'autres secteurs ont été durement touchés également.

Regardez ces statistiques :

- 69 % des entreprises ont été compromises par un rançongiciel en 2020.
- Seuls 8 % des victimes ayant payé la rançon ont récupéré la totalité de leurs données.
- En moyenne, un rançongiciel entraîne un temps d'arrêt de 21 jours. (Certains clients ont signalé des temps d'arrêt beaucoup plus longs.)
- Le coût moyen pour se remettre d'une attaque par rançongiciel est de 1,85 million de dollars.
- En 2020, le coût total des attaques par rançongiciel s'est élevé à 20,8 milliards de dollars, rien que dans le secteur de la santé aux États-Unis !

Cette menace est prise très au sérieux aux niveaux les plus hauts. Les agents officiels de la Maison-Blanche ont envoyé des lettres aux entreprises des États-Unis les incitant à « convoquer immédiatement leurs équipes de direction pour discuter de la menace que représentent les rançongiciels et revoir leur stratégie de sécurité et plans de continuité d'activité en conséquence pour s'assurer de pouvoir continuer leurs activités ou reprendre rapidement les opérations en cas d'attaque ». Le directeur du FBI Christopher Wray a indiqué aux législateurs que cette cybermenace « grandissait de manière quasi exponentielle ». Il a précisé que le gouvernement fédéral conduisait actuellement une enquête sur « 100 variantes de rançongiciels, et que chacune avait fait des dizaines, voire des centaines de victimes ».

69 %

des entreprises ont été compromises par un rançongiciel en 2020, et en moyenne ce type d'attaque entraîne des temps d'arrêt de 21 jours.

Être prêt à payer la rançon n'est pas une stratégie viable.

Le règlement de la rançon n'est pas la réponse. 80 % des victimes ayant payé ont subi une autre attaque par rançongiciel, et près de la moitié d'entre elles (46 %) pense qu'il s'agissait des mêmes auteurs. De plus, le Bureau de contrôle des actifs étrangers (OFAC, Office of Foreign Assets Control) du Département du Trésor des États-Unis a déclaré qu'il était illégal de payer des demandes de rançongiciel dans des cas précis, et a indiqué qu'une entreprise pourrait subir des pénalités, même si elle ne savait pas qu'elle payait (ou qu'elle permettait de payer) une entité non autorisée selon les réglementations OFAC.

Quelle est alors la meilleure voie à suivre ?

Active Directory est la clé de voûte.

Une stratégie complète de prévention des attaques par rançongiciel comprend plusieurs aspects. Il s'agit de réduire la surface d'attaque tout en assurant une détection et une réponse rapides en cas d'attaque. Ce livre blanc aborde un aspect essentiel de cette stratégie : la restauration. Il est crucial de vous assurer que vous pourrez restaurer les opérations métiers aussi rapidement que possible en cas d'attaque par rançongiciel.

La plupart des entreprises utilisent Active Directory (AD) pour gérer les identités et fournir un accès à leurs ressources, comme les bases de données, les fichiers, les applications et les terminaux. Par conséquent, AD est la clé de voûte d'une restauration rapide en cas d'attaque par rançongiciel. D'après un analyste de Gartner : « Le processus de restauration suite à de nombreuses attaques par rançongiciel bien documentées a été entravé par l'absence d'un processus de restauration d'Active Directory intact ».[1]

> Le processus de restauration suite à de nombreuses attaques par rançongiciel bien documentées a été entravé par l'absence d'un processus de restauration d'Active Directory intact.

Gartner, Inc., « How to Recover From a Ransomware Attack Using Modern Backup Infrastructure », Fintan Quinn, 4 juin 2021.

En effet, sans AD, tout le reste s'effondre. C'est pourquoi, pendant la fameuse attaque NotPetya de 2017, un membre de l'équipe informatique de Maersk a indiqué : « Si nous ne pouvons pas restaurer nos contrôleurs de domaine, nous ne pouvons rien récupérer du tout ».[2]

Malheureusement, les solutions de sauvegarde et de restauration traditionnelles peuvent restaurer les identités, mais elles sont incapables d'exécuter une resynchronisation. En d'autres termes, un grand nombre de tâches manuelles doit être effectué sur chaque serveur d'identité, ralentissant considérablement le délai de reprise d'activité. La solution Quest Recovery Manager for Active Directory Disaster Recovery Edition (RMAD DRE), quant à elle, vous permet de vous assurer que vous pourrez reprendre vos activités rapidement et en toute sécurité. L'un de nos clients a gentiment accepté de partager son expérience avec RMAD DRE dans le cadre d'une restauration après une attaque par rançongiciel. Voici les quatre leçons qu'il a apprises.

Étude de cas : une réponse efficace aux rançongiciels

Un rançongiciel a compromis 17 contrôleurs de domaine et presque tous les comptes utilisateur.

Un rançongiciel a récemment infecté un client international du secteur de la fabrication, affectant 17 contrôleurs de domaine sur plusieurs continents. L'attaque a également brouillé les mots de passe Active Directory de 98 % des comptes utilisateur, y compris ceux d'un nombre incalculable de comptes de service.

Au départ, aucun des 17 contrôleurs de domaine ne semblait affecté. Mais après en avoir isolé un sur le réseau, l'équipe informatique a découvert des fichiers chiffrés dans SYSVOL. Ils auraient pu simplement avoir été répliqués à partir d'un autre contrôleur de domaine, mais puisque les rançongiciels aiment se propager via des stratégies de groupe, il était primordial de s'assurer que le logiciel malveillant ne se cachait pas ailleurs sur le serveur. Par conséquent, l'équipe a dû restaurer son réseau et le protéger contre une éventuelle réinfection par la même occasion. Une tâche intimidante, mais ce sont les véritables exigences d'une restauration post-rançongiciel.

C'est là que Quest intervient.

Heureusement, l'entreprise a pu faire appel à Recovery Manager for Active Directory Disaster Recovery Edition. Cette solution lui a donné la flexibilité nécessaire pour utiliser plusieurs méthodes de restauration, y compris une restauration progressive et la restauration d'AD sur un système d'exploitation propre pour minimiser le risque de réinfection par un logiciel malveillant. Avec RMAD DRE, l'équipe de restauration a bénéficié d'un plus grand contrôle sur l'intégralité du processus de reprise d'activité : elle a gagné du temps et économisé des ressources en éliminant les dépendances liées aux équipes interservices.

D'après le chef de projet du service de conseil sur site, « Le client se sentait désemparé jusqu'à ce que Quest intervienne et prenne les choses en main. Le client a immédiatement commencé à reprendre espoir. »

[1] Gartner, Inc., « How to Recover From a Ransomware Attack Using Modern Backup Infrastructure », Fintan Quinn, 4 juin 2021.
[2] Wired Magazine, « The Untold Story of the NotPetya, the Most Devastating Cyberattack in History », https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Une restauration progressive a permis de remettre en service les cinq contrôleurs de domaine prioritaires en moins de deux heures.

Avec RMAD DRE, la société a entrepris une restauration progressive, qui lui a permis de choisir l'ordre de récupération des contrôleurs de domaine, ce afin de laisser les services stratégiques démarrer les opérations de reprise plus rapidement. Tout d'abord, tous les comptes utilisateurs affectés ont été restaurés à partir d'une sauvegarde effectuée cinq jours auparavant. RMAD DRE a même permis à l'équipe de réinitialiser les mots de passe de tous les comptes à privilèges : un facteur essentiel, sachant qu'elle pensait qu'au moins l'un de ces comptes avait été compromis.

Avec RMAD DRE, l'entreprise a pu restaurer cinq contrôleurs de domaine principaux en moins de deux heures, ce qui lui a permis de commencer à remettre les applications stratégiques en ligne.

La restauration s'est ensuite poursuivie ainsi :

- **Phase 1 —** Le premier contrôleur de domaine a été restauré en une heure.
- **Phase 2 —** Le deuxième contrôleur a été restauré en 12 minutes.
- **Phase 3 —** Trois autres contrôleurs de domaine ont été restaurés en 36 minutes dans deux continents.

À ce stade, il y avait suffisamment de ressources dans Active Directory pour commencer à se concentrer sur la remise en ligne de leurs applications métiers. La restauration des contrôleurs de domaine moins essentiels a été programmée à des phases ultérieures.

Ce qu'il faut retenir, c'est que l'entreprise a considérablement réduit son temps d'inactivité avec RMAD DRE, à tel point que le chef de projet s'est montré dithyrambique : « Jamais la restauration n'aurait été si rapide sans l'outil Quest ! »

Cet exemple réel d'une attaque par rançongiciel et de la restauration qui en a suivi a révélé plusieurs leçons importantes dont les entreprises devraient tenir compte pour l'élaboration de leur stratégie de défense contre de telles attaques. Passons-les en revue.

Leçon n° 1. Isolez vos sauvegardes AD.

C'est simple : vous ne pouvez pas effectuer de restauration à partir d'une sauvegarde corrompue. Dans cette logique, de nombreuses attaques par rançongiciel consistent à rechercher activement et à détruire toutes les sauvegardes liées au réseau afin de maximiser les probabilités que vous choisissiez de payer la rançon pour restaurer vos données.

Par conséquent, il est essentiel de ne pas se contenter de faire des sauvegardes régulières et fiables de votre Active Directory : il s'agit également de les conserver dans un stockage isolé. En d'autres termes, hors ligne : déconnectées et inaccessibles depuis Internet et les réseaux internes.

La solution traditionnelle consistait à écrire les sauvegardes sur bande et à les envoyer dans une installation de stockage hors site comme Iron Mountain. Mais cette approche, qui a déjà l'inconvénient d'être compliquée et coûteuse, ralentit considérablement la restauration. En effet, la récupération, le transport, le montage et la lecture des bandes prend énormément de temps. Cela peut avoir une incidence énorme sur le respect de votre RTO (objectif de délai de restauration) : si vous utilisez un stockage physique hors site, nous ne saurions trop vous conseiller de revoir vos contrats de niveau de service (SLA). Aujourd'hui, nombre d'entreprises explorent les solutions Cloud pour le stockage de leurs sauvegardes. Ces solutions incluent : Amazon Simple Storage Service (Amazon S3) (plus S3 Glacier et S3 Glacier Deep Archive) et le stockage immuable de Microsoft Azure Blob.

Avec RMAD DRE cependant, il est inutile d'avoir recours à une solution de stockage distincte. Depuis la version 10.2, la solution inclut un serveur de stockage sécurisé. Il s'agit d'un serveur hautement protégé par des pare-feu qui n'autorise pratiquement aucun accès : pas de ping, pas de RDP, pas de PC, pas de bureaux à distance, pas de partages SMB. Les ports SMB ne sont pas simplement désactivés, ce sont ces protocoles qui sont directement désactivés sur le serveur de stockage sécurisé. Le seul moyen d'y accéder est d'utiliser un port TCP utilisant un chiffrement TLS que vous pouvez définir. Ce port TLS est utilisé pour notifier l'agent de stockage de la création d'une sauvegarde sur le stockage de niveau 1, ce qui permet à l'agent de collecter la sauvegarde elle-même. En d'autres termes, les pare-feu ne tombent jamais. En outre, la solution vérifie l'intégrité de chaque sauvegarde.

Pour sortir une sauvegarde, vous devez vous rendre physiquement dans le datacenter pour vous connecter à la console. Même si cela peut paraître peu commode, cette exigence fait qu'il est pratiquement impossible pour l'auteur de l'attaque par rançongiciel de compromettre les sauvegardes. Avec cette sauvegarde sécurisée, RMAD DRE peut restaurer Active Directory sur un nouveau serveur, pour démarrer rapidement la reprise.

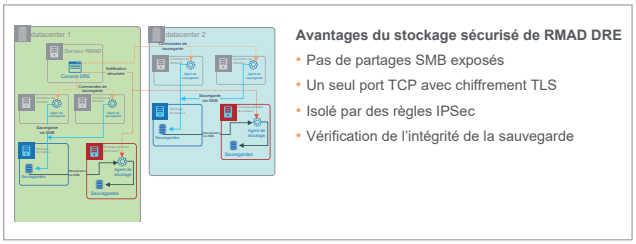

Figure 1. Le serveur de stockage sécurisé de RMAD DRE propose un stockage isolé pour protéger les sauvegardes AD contre les rançongiciels

Leçon n° 2. Établissez un plan pour les attaques par rançongiciel et TESTEZ-LE !

La restauration de forêts est un processus complexe qui implique plus de 40 étapes par contrôleur de domaine à récupérer à partir de la sauvegarde. De ce fait, il est judicieux d'avoir à sa disposition une solution automatisée et un plan documenté testé régulièrement. Assurez-vous que votre plan prévoit spécifiquement la restauration d'AD en cas d'attaque par rançongiciel. Trop d'entreprises font l'erreur de se concentrer uniquement sur la restauration des applications, mais votre plan doit prévoir que vous n'aurez plus de contrôleurs de domaine pour exécuter ces applications.

> Ne faites pas l'erreur de vous concentrer uniquement sur la restauration des applications : votre plan doit prévoir que vous n'aurez plus de contrôleurs de domaine sur lesquels exécuter les applications.

Nommez un chef et délimitez bien les responsabilités de chacun.

Une procédure de restauration fait intervenir un certain nombre d'équipes, comme :

- Une **équipe Sauvegarde** qui fournit les sauvegardes et effectue les restaurations
- Une **équipe Stockage** qui garantit que vous disposez d'un espace suffisant pour restaurer les serveurs à partir de la sauvegarde
- Une **équipe Réseau** qui veille à ce que les serveurs restaurés soient mis en sandbox et que les contrôleurs de domaine puissent communiquer
- Une **équipe Serveur** qui vérifie la réussite de la restauration et qui installe les logiciels antivirus ou anti-logiciels malveillants éventuellement requis
- Une **équipe Sécurité** qui vérifie que le rançongiciel ne se trouve pas sur les serveurs restaurés
- Une **équipe Application** qui vérifie que les applications fonctionnent
- Des **parties externes**, comme Microsoft, votre fournisseur de solution de sauvegarde et de restauration, et votre fournisseur de stockage Cloud

Il est primordial de nommer un responsable qui dirigera et coordonnera toutes ces équipes, et qui prendra les décisions à la volée. Veillez également à avoir clairement documenté l'ensemble des rôles et des responsabilités.

Créez une cellule de crise virtuelle.

Votre guide de défense contre les rançongiciels devrait également inclure une cellule de crise virtuelle où toutes ces équipes pourront se réunir. Prévoyez un moyen de les scinder en petits groupes dans des salles virtuelles distinctes pour réfléchir à des stratégies concernant des problèmes spécifiques. Zoom et Microsoft Teams peuvent faire l'affaire, mais l'application Teamflow est également un choix envisageable.

Ne limitez pas votre plan à la restauration d'AD.

N'oubliez pas que la restauration d'AD n'est pas la seule tâche à accomplir en cas d'attaque par rançongiciel. Pensez à son impact sur votre réseau, vos routeurs et vos commutateurs. Pensez également à la manière dont vos concentrateurs VPN communiquent avec votre annuaire. En outre, vous voudrez également peut-être améliorer vos serveurs en renforçant leur sécurité, et en installant des logiciels de détection et de réponse.

Veillez à ce que votre plan soit accessible.

Pensez à stocker votre plan dans un emplacement auquel vous pourrez accéder même en cas de sérieuse attaque par rançongiciel. L'impression de ce plan est une tactique qui a fait ses preuves, mais vous pouvez également choisir de le conserver dans un stockage Cloud séparé, comme Dropbox.

Leçon n° 3. Envisagez une restauration progressive.

Comme indiqué plus tôt, l'entreprise de fabrication internationale de notre exemple a effectué une restauration progressive : elle a commencé par restaurer les contrôleurs de domaine les plus stratégiques, ce qui lui a permis de reprendre presque immédiatement ses activités.

Commencez par identifier les applications les plus essentielles au bon fonctionnement des opérations métiers, afin de pouvoir vous concentrer sur leur restauration en priorité. Identifiez ensuite les contrôleurs de domaine indispensables à ces applications. Bien souvent, les contrôleurs de domaine clés sont ceux qui se trouvent dans le datacenter plutôt que dans les bureaux distants. Une fois ces contrôleurs restaurés, les équipes chargées des applications, des bases de données et d'autres, peuvent démarrer leur propre processus de restauration pendant que l'équipe Active Directory commence à restaurer les contrôleurs de domaine moins essentiels. La figure 2 illustre la stratégie de restauration progressive.

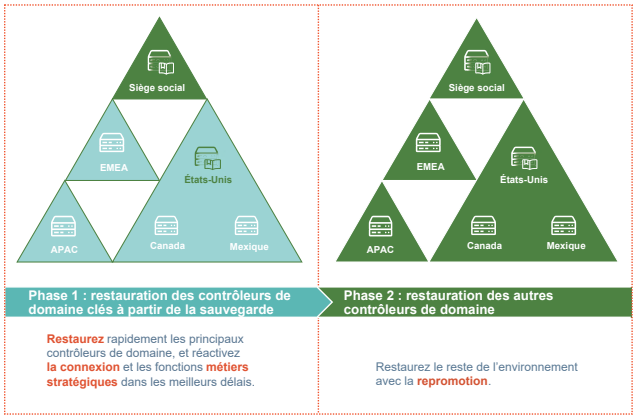

Figure 2. Une restauration progressive peut vous aider à remettre vos processus métiers stratégiques en ligne rapidement.

Leçon n° 4. Il ne s'agit pas uniquement d'effectuer une restauration rapide.

En revanche, rappelez-vous que la reprise post-rançongiciel n'est pas une course. Il s'agit également de s'assurer que la restauration est bien faite et que vous ne risquez pas de vous faire réinfecter. RMAD DRE réduit ce risque en vous donnant la possibilité de choisir le meilleur moyen de restaurer chacun de vos contrôleurs de domaine :

- **Restauration sans système d'exploitation :** restaurez tous les volumes de votre contrôleur de domaine sur un autre matériel
- **Restauration sur un système d'exploitation vierge :** restaurez AD sur un nouveau Windows Server tout en réduisant le risque de réinfection
- **Installation d'Active Directory :** promouvez de nouveaux serveurs qui viendront remplacer les contrôleurs de domaine que vous n'avez pas restaurés à partir de la sauvegarde
- **Désinstallation d'Active Directory :** forcez la rétrogradation d'un contrôleur de domaine et supprimez toutes les métadonnées associées dans l'annuaire
- **Réinstallation d'Active Directory :** forcez la rétrogradation des contrôleurs de domaine et repromouvez-les lorsque le système d'exploitation est toujours intact
- **Restauration d'AD à partir d'une sauvegarde :** restaurez AD sur un serveur sain
- **Repromotion :** promouvez le reste des contrôleurs de domaine dans une forêt partiellement restaurée

Au moment de faire votre choix, comprenez bien que la restauration sans système d'exploitation nécessite que votre machine cible ait la même configuration de disque physique que le contrôleur de domaine d'où provient la sauvegarde. De plus, la sauvegarde inclut des composants qui ne sont pas nécessaires pour l'opération de restauration, comme le volume de démarrage : autant d'emplacements où le rançongiciel peut se cacher pour réinfecter votre entreprise.

L'option de restauration sur un système d'exploitation vierge dans RMAD DRE réduit considérablement ce risque, car la sauvegarde inclut uniquement les informations requises (cf. Figure 3). En outre, RMAD DRE peut également analyser les sauvegardes à la recherche de logiciels malveillants avant de les utiliser pour la restauration. La solution peut également réinitialiser les mots de passe des membres des groupes à privilèges intégrés pendant l'opération de restauration. De plus, RMAD DRE vous permet de restaurer AD sur une machine virtuelle Microsoft Azure. Vous avez la certitude que vous restaurez AD sur une machine disponible, sécurisée et économique, sans aucun logiciel malveillant.

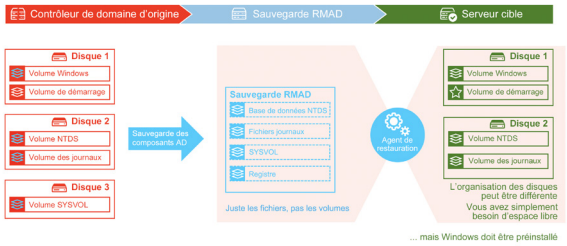

Figure 3. L'option de restauration sur un système d'exploitation vierge de RMAD DRE réduit considérablement le risque d'infection pendant le processus de restauration

Conclusion

Aujourd'hui, chaque entreprise doit avoir une stratégie complète de réponse à une attaque par rançongiciel qui lui permettra de restaurer rapidement ses contrôleurs de domaine clés et de reprendre son activité dans la foulée. Recovery Manager for Active Directory Disaster Recovery Edition peut être un composant très utile dans ce cadre. Cette solution a aidé une entreprise internationale du secteur de la fabrication à restaurer ses cinq contrôleurs de domaine les plus stratégiques en moins de deux heures, ce qui lui a permis de commencer la restauration des applications et bases de données essentielles pour reprendre les opérations principales.

Pour en savoir plus, rendez-vous à la page https://www.quest.com/products/recovery-manager-for-active-directory-disaster-recovery-edition/.

Quest

Profil de Quest

Quest créé des solutions logicielles conçues pour exploiter tous les avantages des nouvelles technologies dans un paysage informatique toujours plus complexe. De la gestion des bases de données et des systèmes à celle d'Active Directory et d'Office 365, en passant par la cybersécurité et la résilience, Quest aide ses clients à relever leurs prochains défis informatiques dès à présent. Partout dans le monde, plus de 130 000 entreprises et 95 % de celles du classement Fortune 500 font confiance à Quest pour assurer une gestion et une surveillance proactives afin de soutenir toute nouvelle initiative, de surmonter les défis Microsoft complexes et de garder une longueur d'avance sur les menaces à venir. Quest Software. Where Next Meets Now.

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :
www.quest.com/fr-fr/company/contact-us.aspx